

FILED ENTERED
LODGED RECEIVED

JUN 17 2013

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON DEPUTY
RY

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

NIKOLA KOVACEVIC,
a.k.a. "Serbian,"

Defendant.

CASE NO.

COMPLAINT for VIOLATION

18 U.S.C. §§ 1029(a)(1) and 2

18 U.S.C. § 1028A

BEFORE the Honorable James P. Donohue, United States Magistrate Judge, U.S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT 1
(Access Device Fraud)

On or about February 2, 2013, at Seattle, within the Western District of Washington, the defendant, NIKOLA KOVACEVIC, knowingly, and with intent to defraud, did use a counterfeit access device, to wit: a counterfeit card encoded with account information belonging to a real person, to withdraw, and attempt to withdraw, cash from an automated teller machine; said conduct affecting interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 1029(a)(1) and 2.

COUNT 2
(Aggravated Identity Theft)

On or about February 2, 2013, at Seattle, within the Western District of Washington, the defendant, NIKOLA KOVACEVIC, did knowingly transfer, possess and use, without lawful authority, the means of identification of another person, that is, the personal identification number (PIN) and account number and information belonging to a real person, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), that is, Access Device Fraud, in violation of Title 18, United States Code, Section 1029(a), as charged in Count 1, above, as well as Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Bank Fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Section 1028A(a).

And the complainant states that this Complaint is based on the following information:

I, John Wurster, being first duly sworn on oath, depose and say:

I. BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so since June 21, 1999. I am currently assigned to the Seattle Field Office. I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the United States Secret Service, Special Agent Training Program located in Beltsville, Maryland. Prior to my employment with the Secret Service, I served in the United States Army as a Counterintelligence Special Agent. I have a Bachelor of Science Degree from Brenau University. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud and identity theft. I have also completed specialized training in the investigation of electronic crimes involving the use of computers and other electronic devices. In the course of my law enforcement career, I have investigated crimes ranging from the production and passing of counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the President and Vice President of the United States. As part of my duties, I also investigate

II. INVESTIGATION

A. Background: Skimming and Skimming Devices

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

1 data, of an unsuspecting victim's credit/debit card. Skimming devices are often capable of
2 holding data pertaining to hundreds or even thousands of bank cards.

3 5. After stealing card data, suspects will transfer the victim account data to a
4 computer or other electronic storage device. Typically, suspects will then transfer or "re-code"
5 victim card data onto blank credit/debit card stock, also known as "white plastic." Suspects have
6 also been known to re-code stolen card data onto store gift cards or other credit/debit cards.
7 Virtually any plastic card with a magnetic stripe on the back of the card may be used to re-code
8 victim card data and in turn to access funds and/or credit on the victim's account. Given the
9 nature of the activity, skimming necessarily requires use of a computer and other digital devices,
10 including encoding equipment and software and USB devices.

11 6. Once this process is complete, suspects use the newly made counterfeit cards,
12 sometimes called "white plastic cards," to access victim's accounts. Typically, suspects will use
13 victim information to withdraw cash at ATMs, which also requires the use of victims' personal
14 identification number (PIN), and/or to make point-of-sale purchases within a short period of time
15 from the date that the credit/debit card account was "skimmed." In some instances, however,
16 suspects will wait several months before utilizing the stolen data. In either case, however,
17 suspects will typically conduct numerous fraudulent transactions in a short time frame in order to
18 maximize the use of the stolen data before the financial institutions or the individual victim
19 account holders recognize the breach and begins shutting down the compromised accounts.

20 **B. Evidence of Criminal Activity**

21 7. This investigation originated on December 9, 2012, when a Boeing Employees
22 Credit Union (BECU) Investigator identified a group of individuals performing "cash outs" —
23 that is, mass fraudulent cash withdrawals — at BECU ATMs in and around Seattle. BECU
24 gathered surveillance photos and a list of card numbers being used at BECU ATMs. An
25 examination of the card numbers revealed that they all related to debit cards and accounts at
26 VanCity Credit Union of Vancouver, British Columbia.

27 8. The United States Secret Service (USSS) Vancouver Resident Office contacted
28 VanCity investigators concerning the debit cards used in and around Seattle at the BECU ATMs

1 and it was determined that these cards had been compromised from various coffee shops in
2 Vancouver.

3 9. Following this initial video dump from BECU, it appeared that the same
4 individuals were performing cash outs in Seattle on a regular basis, predominantly using
5 Canadian bank card numbers. One recurring suspect was a male later identified as NIKOLA
6 KOVACEVIC. The cash out dates typically were on weekends, such as the weekends of
7 December 1, 2012; December 9, 2012; January 5, 2013; January 20, 2013; and February 2, 2013.
8 According to the Royal Canadian Mounted Police (RCMP), it has verified at least 11 common
9 points of purchase believed to have been compromised through card skimming activity, where
10 customers' card data and their PINs had been stolen through the use of skimming devices.

11 10. On January 5, 2013, the RCMP contacted the USSS Vancouver Resident Office
12 requesting assistance with the investigation of T.M., a Canadian citizen. The Canadian Border
13 Services Agency had intercepted T.M. with 22 "white plastic cards" containing TD Bank data
14 and \$12,000.00 in cash at the Douglas Border Crossing. Inside T.M.'s phone was the name
15 "Dennis." According to Canadian authorities, "Dennis" was identified as "Dennis Nguyen," a
16 Canadian citizen residing in British Columbia. They also reported finding several phone
17 numbers for area codes in Washington State.

18 11. According to border crossing records, Dennis Nguyen made at least eight border
19 crossings from Canada into the United States since November 2012. In each instance he was
20 driving the same 2008 Jeep Cherokee with a British Columbia license plate.

21 12. On February 5, 2013, the USSS Seattle Field Office was notified that the Royal
22 Bank of Canada (RBC) reported a mass cash out attempt in progress at numerous ATMs in the
23 downtown Seattle area. RBC provided real time data of where the transactions were taking
24 place, which enabled JP Morgan Chase Bank central fraud monitoring to provide a photograph
25 and description of a suspect. Surveillance videos showed the suspect, a Hispanic male with dark,
26 spiked hair, wearing a black jacket and jeans, conducting the cash-outs at various ATMs.

27 13. A search of the areas near these ATMs was initiated. Detective David Dunn of
28 the Seattle Police Department and USSS Special Agent Bryan Molnar located the suspect at an

1 ATM on 4th Ave in Westlake Park in downtown Seattle. The suspect, identified as Santiago
2 Zayco, was contacted and taken into custody. A search incident to arrest yielded 49 "white
3 plastic cards" and \$1,620.00 in cash wrapped around ATM receipts from Zayco's person. It
4 should be noted the "white plastic cards" had no bank markings or printing on the front or back,
5 just a magnetic strip. A white label was printed on the front of each card with what appeared to
6 be a four-digit PIN on each. I know from my training, experience and other investigations that
7 "white plastic cards" are used by skimmers and other types of fraud suspects to encode
8 information and then withdraw money or purchase items.

9 14. Santiago Zayco was transported to the USSS Seattle Field Office, where he agreed
10 to be interviewed. Agent Molnar read Zayco his Miranda Rights, which Zayco stated he
11 understood. Zayco agreed to speak with law enforcement. Agent Molnar asked Zayco how he
12 had traveled downtown and asked if he was alone. Zayco stated he was alone at the time we
13 contacted him, but his cousin's husband was coming to the area to do cash outs with him. Agent
14 Molnar asked Zayco for consent to search his car and read him a "consent to search" form.
15 Zayco agreed and signed the consent form. Zayco informed Agent Molnar his car was parked
16 underneath the Pacific Place Mall in the parking garage, on the lowest level.

17 15. USSS Special Agent Malcolm Frederick and I located Zayco's vehicle, where
18 Zayco had described, and initiated the search. Inside Zayco's vehicle, Agent Frederick and I
19 found 169 white plastic credit cards and \$6,340.00 in cash wrapped around ATM receipts. While
20 we were searching the car, Agent Frederick observed a male driving a black Mercedes watching
21 us as he slowly drove through the parking garage.

22 16. Upon completion of the search, I advised Agent Molnar of the results. During
23 subsequent questioning, Agent Molnar asked Zayco about the items found in the car. Zayco
24 admitted the money found in the car was obtained from the illegal cash out scheme and the white
25 plastic cards were provided to him by "Dennis" to do the cash outs. Zayco said he would meet
26 with "Dennis" every week or two. "Dennis" would give him new cards and Zayco would give
27 "Dennis" the cash he obtained from doing cash-outs with the prior week's cards, along with the
28 corresponding ATM receipts. Zayco said he would be given a portion of the cash from the cash

1 outs as payment. Zayco said he corresponded with "Dennis" by a "burner" cellular telephone that
2 "Dennis" would provide him. I know from my training and experience that individuals involved
3 in criminal activities may utilize pre-paid cellular phones due to the anonymity such devices may
4 provide. These phones do not require a contract with a telephone service provider that could be
5 researched for account billing information. Instead, following the initial cash purchase of such a
6 phone at any number of retail stores, these phones may be loaded with minutes and/or days of
7 service via the cash purchase of gift cards associated with the provider of the cell phone. The
8 terms "burner " and "burn phone" are related to the ease with which suspects can discard such
9 phones if they believe they may be arrested or "burned."

10 17. Zayco was shown a surveillance photograph of Dennis Nguyen, provided by the
11 USSS Vancouver Resident Office, and Zayco identified Nguyen as the person known to him as
12 "Dennis." Zayco also was shown surveillance photos of himself and other people in this group
13 using cards encoded with stolen account information to make cash outs. Zayco identified, among
14 others, himself and his cousin's husband, Chris Rolon-Gonzales (Rolon), performing cash outs at
15 ATMs with counterfeit cards and stolen PINs.

16 18. Later the same day, Chris Rolon was taken into custody and, after being read and
17 and stating he understood his Miranda Rights, also agreed to be interviewed. Rolon further gave
18 written consent to a search of his vehicle. Agent Molnar asked Rolon if there was any
19 contraband in the vehicle. Rolon stated we would find cash in the car. I asked him where he
20 obtained the money, and Rolon admitted it was from doing cash outs. While conducting the
21 search of Rolon's vehicle, USSS Special Agent David Mills and Agent Frederick located
22 \$4,760.00 in cash and ATM receipts hidden in a gym bag in the trunk of the car.

23 19. During the interview, Rolon admitted to doing the cash outs for "Dennis" who he
24 had met through a "cousin's cousin" named T.M. (same as above). Rolon was shown a
25 surveillance photograph of Dennis Nguyen, provided by the USSS Vancouver Resident Office,
26 and Rolon identified Nguyen as the person known to him as "Dennis."

27 20. Rolon stated he and Zayco typically would meet with Nguyen every week or two.
28 Rolon said he and Zayco would share a cell phone in which they would communicate with

1 Nguyen through text messages and calls. Rolon said they typically met at hotel rooms on the
2 west side of Interstate 5 near Northgate Mall, where Nguyen gave them counterfeit cards. Rolon
3 was shown photographs of other people doing cash-outs. Rolon identified Zayco as well as
4 others.

5 21. Rolon and Zayco later provided to USSS agents a red duffle bag that Dennis
6 Nguyen left with them, which they provided to Nguyen when he traveled to Washington from
7 Canada. A search of that bag yielded \$77,140.00 in cash, about 462 plastic cards (most of which
8 were encoded with account data and had a printed label with the associated 4-digit PIN), seven
9 "burner" cell phones of the same make and model, a cash counting machine, a credit card
10 magnetic strip encoder, a label printer, label printing software, 12 rolls of white label tape, and
11 miscellaneous supplies. Based upon my training, experience and my examination of the
12 evidence contained in the red bag, I know the credit card magnetic strip encoder, "white plastic
13 cards", label printer and blank labels are used in the production of counterfeit access devices.

14 22. On February 11, 2013, Dennis Nguyen, and a female associate, crossed the border
15 into the United States and traveled to the Seattle area where he had arranged to meet Zayco and
16 Rolon to pick up the red duffle bag. Nguyen was arrested in a parking lot near Northgate Mall.
17 In Nguyen's vehicle was, among other things, a laptop computer. A forensic analysis of that
18 computer identified about 3,000 credit/debit card account numbers, belonging to customers of
19 various domestic and foreign financial institutions, on the hard drive. Hundreds of those card
20 numbers matched those encoded on seized counterfeit cards.

21 23. Dennis Nguyen was advised of his Miranda rights, which he stated he understood,
22 and agreed to be interviewed. Nguyen admitted to his involvement in criminal activity involving
23 counterfeit cards. Nguyen, however, claimed that he was primarily a deliveryman and was
24 supposed to meet and provide cash, cards, and equipment to another person he called "Morocco"
25 — the person, according to Nguyen, who actually made the counterfeit cards. Nguyen described
26 "Morocco" as a black male, about 6-feet tall and 205 pounds, with short black hair. During the
27 interview of Nguyen, a "burner" cell phone discovered on Nguyen's person rang periodically.
28

1 Nguyen explained that he was supposed to meet up with "Morocco" who was traveling to Seattle
2 from Canada.

3 24. I later reviewed incoming and outgoing text messages from the "burner" cell
4 phone recovered from Dennis Nguyen's person. The following incoming messages were
5 received by Nguyen on February 11, 2013:

<u>Date/Time</u>	<u>Text Message</u>
2/11/13 @ 1621:	"6047167596"
2/11/13 @ 2015:	"Yo Im here"
2/11/13 @ 2120:	"Yo im at the same hotel as usual. 223"

6
7
8
9 25. On February 21, 2013, I interviewed Chris Rolon as part of a non-custodial
10 interview. Rolon was shown a collection of ATM surveillance photos associated with this
11 investigation and, among others, he identified a white male whom he referred to as "Serbian" and
12 a black male whom he referred to as "Morocco." When questioned, Rolon also explained in
13 greater detail how he became involved in the scheme. He said that T.M., who resides in Canada,
14 had called him about mailing to Rolon a package that someone would come by to pick up. Rolon
15 said that he was not home when that package arrived, but Santiago Zayco was present. He said
16 Zayco later told him that two males came by and picked up the package. Rolon said Zayco told
17 him these two males wanted to meet to discuss a way to make some money.

18 26. Rolon said that the following day he and Zayco met with the two males he
19 previously identified as "Morocco" and "Serbian." He said he believed that "Morocco" and
20 "Serbian" were Canadian, because the vehicle they were driving (an unknown Volkswagon
21 model) had Canadian license plates. Rolon said "Morocco" and "Serbian" described how he and
22 Zayco could earn money by performing ATM withdrawals. "Morocco" and "Serbian" told them
23 to visit a Days Inn hotel on Aurora Avenue in Seattle later that day, which Rolon and Zayco did.
24 Rolon said there were approximately ten people in the hotel room and that "Morocco" and
25 "Serbian" were leaving as he and Zayco arrived. Rolon said that he and Zayco spoke with
26 Dennis Nguyen, who said he initially gave them five cards with PINs printed upon them and
27 instructed them on how to use the cards to withdraw money from ATMs.
28

27. On February 27, 2013, Special Agent Bryan Molnar and I also interviewed Santiago Zayco. Zayco was shown a collection of ATM surveillance photos associated with this investigation and also identified the two males known to him as "Serbian" and "Morocco." Zayco also recounted "Serbian" and "Morocco" coming to Rolon's house for the package as well as his and Rolon's later meetings with them and also with Nguyen, which was consistent with what Rolon had previously told agents.

28. On March 14, 2013, I interviewed receptionists at hotels in the areas Santiago Zayco and Christopher Rolon-Gonzales said they met with Dennis Nguyen. I confirmed that Dennis Nguyen stayed at the following locations on the following dates:

<u>Check-In/Out</u>	<u>Hotel/Address</u>
December 2-3, 2012	Travelodge/8512 Aurora Ave N, Seattle, WA
December 9-10, 2012	Days Inn/9100 Aurora Ave N, Seattle, WA
December 10-12, 2012	Hotel Nexus/2140 N Northgate Way, Seattle, WA
January 8-13, 2013	Hotel Nexus/2140 N Northgate Way, Seattle, WA
January 29, 2013	Tulalip Resort/10200 Quilceda Blvd, Tulalip, WA
February 2-5, 2013	Hotel Nexus/2140 N Northgate Way, Seattle, WA

Upon reviewing this information, I recalled the following text message that was received on the "burner" cell phone seized from Dennis Nguyen when he was arrested on February 11, 2013:

<u>Date/Time</u>	<u>Text Message</u>
2/11/13 @ 2120:	"Yo im at the same hotel as usual. 223"

29. On March 15, 2013, I interviewed a particular Concierge/Guest Receptionist, Hotel Nexus, 2140 N Northgate Way, Seattle, Washington. When questioned, the receptionist said that a man, K.H., rented room 223 on February 11, 2013. She said she recalled this transaction, because K.H. later asked for a refund and checked out of the hotel during the early hours of February 12, 2013. The receptionist provided me with a note which was attached to this transaction record, which stated "guest checked in expecting his friends to make it across the border for their vacation but they got denied, he didn't touch the room so therefore I refunded him due to it not being an inconvenients to us, thanx! . . ."

30. When I asked if K.H. had rented rooms at the Hotel Nexus prior to February 11, 2013, the receptionist provided the following information:

<u>Check-In/Out</u>	<u>Primary Guest/Secondary Guest</u>
December 11-17, 2012	[C.V.]/[K.H.]
February 3-4, 2013	[K.H.]/(none listed)

1 According to records, K.H. provided a Vancouver, BC address.

2 31. Later that same day, I provided information regarding K.H. and C.V. to SA John
3 Liau, USSS, Vancouver Resident Office.

4 32. On March 18, 2013, I spoke with SA Liau, who said he provided the above
5 information regarding K.H. and C.V. to the RCMP. He said the RCMP reported that K.H. has a
6 grey Volkswagen Passat registered to him. I recalled my interview of Chris Rolon, during which
7 he said the individuals he identified as "Morocco" and "Serbian" were possibly Canadian,
8 because the vehicle they were driving (an unrecalled Volkswagen model) had Canadian license
9 plates. SA Liau said he would contact Homeland Security Investigations/U.S. Immigration and
10 Customs Enforcement (HSI/ICE) and request border crossings, associates, and vehicle
11 information for K.H. and C.V.

12 33. Later that same day, SA Liau provided me a HSI/ICE report detailing the
13 U.S./Canadian border crossings of K.H. and individuals who crossed the border with him. The
14 report provided that K.H. entered the United States from Canada on March 16, 2013, March 8,
15 2013, February 11, 2013, February 2, 2013, January 5, 2013, November 30, 2012, September 25,
16 2012, September 24, 2012, September 20, 2012, September 2, 2012, August 5, 2012, August 4,
17 2012, July 26, 2012, July 22, 2012, March 22, 2012, March 5, 2012, February 29, 2012, February
18 16, 2012 and October 29, 2011. Upon further review, I noticed that an individual named
19 NIKOLA KOVACEVIC crossed the border with K.H. on February 2, 2013, January 5, 2013,
20 November 30, 2012, August 4, 2012 and July 22, 2012.

21 34. The report provided several photographs associated with these border crossings.
22 Upon reviewing photographs taken on February 2, 2013, January 5, 2013, November 30, 2012
23 and July 22, 2012, I identified K.H. as the individual whom both Santiago Zayco and Christopher
24 Rolon-Gonzales previously identified as "Morocco" from ATM surveillance photographs. I also
25 identified NIKOLA KOVACEVIC as the individual whom both Zayco and Rolon identified as
26 "Serbian" from ATM surveillance photographs. Moreover, on February 2, 2013, January 5, 2013
27
28

1 and November 30, 2012, K.H. and KOVACEVIC crossed the border in a Volkswagen Passat
2 bearing British Columbia license plate 598XMJ.¹

3 35. I reviewed records from hotels in the areas Santiago Zayco and Chris Rolon said
4 they met with Dennis Nguyen. I discovered that NIKOLA KOVACEVIC and K.H. obtained a
5 hotel room at a Days Inn, 9100 Aurora Avenue North, Seattle, Washington, from February 2,
6 2013 to February 3, 2013. I recalled that K.H. and KOVACEVIC had crossed the border into the
7 United States together on February 2, 2013, and that I had previously discovered that K.H. had
8 rented a room at the Hotel Nexus, which is nearby the aforementioned Days Inn, from February 3
9 to February 4, 2013. I also recalled that Dennis Nguyen rented a room at the same Days Inn, on
10 Aurora Avenue, from December 9 to December 10, 2012.

11 36. The border crossing dates of K.H. and NIKOLA KOVACEVIC coincide with
12 ATM surveillance images I have reviewed of K.H. and KOVACEVIC conducting fraudulent
13 cash withdrawals at ATMs in the Seattle area, using stolen PINs and counterfeit cards encoded
14 with stolen account data. Such cash-out activity occurred on numerous dates and at various
15 ATMs. By way of example:

16 a. On December 1, 2012, NIKOLA KOVACEVIC used an access device
17 encoded with financial information and a PIN relating to a card number ending in -3399, to
18 access an Interior Savings Credit Union account belonging to account holder B.T., a real person,
19 to obtain \$380.00 from a BECU ATM located in Seattle, Washington.

20 b. On December 1, 2012, NIKOLA KOVACEVIC used an access device
21 encoded with financial information and a PIN relating to a card number ending in -8409, to
22 access an HSBC Bank of Canada account belonging to account holder R.A., a real person, to
23 obtain \$240.00 from a BECU ATM located in Seattle, Washington.

24 c. On December 1, 2012, K.H. used an access device encoded with financial
25 information and a PIN relating to a card number ending in -5316, to access a Van City Credit
26 Union account belonging to account holder A.B., a real person, and attempted to obtain \$100.00

27
28 ¹ On August 4, 2012, K.H. and KOVACEVIC crossed the border in a Volkswagen Passat
bearing British Columbia license plate 704RLE.

1 from a BECU ATM located in Seattle, Washington.

2 d. On December 1, 2012, K.H. used an access device encoded with financial
3 information and a PIN relating to a card number ending in -5316, to access a Van City Credit
4 Union account belonging to account holder A.B., a real person, to obtain \$20.00 from a BECU
5 ATM located in Seattle, Washington.

6 e. On December 2, 2012, NIKOLA KOVACEVIC used an access device
7 encoded with financial information and a PIN relating to a card number ending in -1088, to
8 access a Gulf and Fraser Fishermen's Credit Union account belonging to account holder J.T., a
9 real person, to obtain \$380.00 from a BECU ATM located in Seattle, Washington.

10 f. On December 2, 2012, K.H. used an access device encoded with financial
11 information and a PIN relating to a card number ending in -2404, to access a HSBC Bank of
12 Canada account belonging to account holder K.W., a real person, and attempted to obtain
13 \$100.00 from a BECU ATM located in Seattle, Washington.

14 g. On December 9, 2012, NIKOLA KOVACEVIC used an access device
15 encoded with financial information and a PIN relating to a card number ending in -9640, to
16 access a Coast Capital Savings account belonging to account holder N.F., a real person, to obtain
17 \$220.00 from a BECU ATM located in Seattle, Washington.

18 h. On January 5, 2013, NIKOLA KOVACEVIC used an access device
19 encoded with financial information and a PIN relating to a card number ending in -9516, to
20 access a Van City Credit Union account belonging to account holder J.S., a real person, to obtain
21 \$380.00 from a BECU ATM located in Seattle, Washington.

22 i. On February 2, 2013, NIKOLA KOVACEVIC used an access device
23 encoded with financial information and a PIN relating to a card number ending in -1604, to
24 access a North Shore Credit Union account belonging to account holder C.C., a real person, to
25 obtain \$380.00 from a BECU ATM located in Seattle, Washington.

26 j. On February 2, 2013, NIKOLA KOVACEVIC used an access device
27 encoded with financial information and a PIN relating to a card number ending in -2227, to
28 access a Coastal Community Credit Union account belonging to account holder J.C., a real

1 person, to obtain \$380.00 from a BECU ATM located in Seattle, Washington.

2 k. On February 2, 2013, K.H. used an access device encoded with financial
3 information and a PIN relating to a card number ending in -0003, to access a HSBC Bank of
4 Canada account belonging to account holder A.A., a real person, and attempted to obtain \$560.00
5 from a BECU ATM located in Seattle, Washington.

6 l. On February 2, 2013, K.H. used an access device encoded with financial
7 information and a PIN relating to a card number ending in -0606, to access a HSBC Bank of
8 Canada account belonging to account holder H.W., a real person, and attempted to obtain
9 \$560.00 from a BECU ATM located in Seattle, Washington.

10 All of the aforementioned transactions caused to be transmitted a wire and a signal that traveled
11 in interstate or foreign commerce. Sample ATM surveillance images of NIKOLA
12 KOVACEVIC conducting cash-out activity using stolen customer information are attached
13 hereto as Exhibit A.

14 37. In total, USSS thus far has recovered about 700 "white plastic cards" and about
15 \$89,860 in cash as part of its investigation. Of those "white plastic cards," at least 677 were
16 encoded with account data and are thus counterfeit cards (or "counterfeit access devices," as
17 defined by federal law). The investigation further has identified about 3,000 credit/debit card
18 numbers belonging to others, presumed victims of card skimming activity. The investigation
19 remains ongoing.

20 //

21 //

22 //

23

24

25

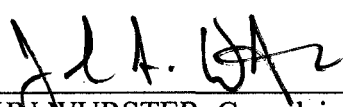
26

27

28

III. CONCLUSION

38. Based on the above facts, I respectfully submit that there is probable cause to believe that NIKOLA KOVACEVIC did knowingly and intentionally commit the offenses of Access Device Fraud, in violation of Title 18, United States Code, Sections 1029(a) and 2, and Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028A.


JOHN WURSTER, Complainant
Special Agent, United States Secret Service

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offense set forth in the Complaint.

Dated this 17th day of June, 2013.

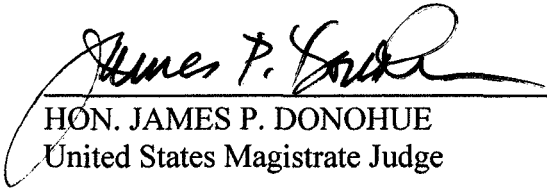

HON. JAMES P. DONOHUE
United States Magistrate Judge

Exhibit A

Transaction #7658
CARD NO: 4761

LOCATION: 1527 2ND AVENUE
SEATTLE WA

CARD NO: XXXXXXXXXXXXX4761

DATE 02/02/13 TIME 08:16PM
TERMINAL WA033861

SEQ NBR: 7658 AMT: \$380.00
ATM OWNER FEE \$2.50
TOTAL \$382.50

CHECKING WITHDRAWAL \$257.85
AVAILABLE BALANCE \$257.85
BALANCE

LOCATION: 1527 2ND AVENUE
SEATTLE WA

CARD NO: XXXXXXXXXXXXX4761

DATE 02/02/13 TIME 08:16PM
TERMINAL WA033861

SEQ NBR: 7658 AMT: \$380.00
ATM OWNER FEE \$2.50
TOTAL



2nd & Pine - NFC-1527-Pine-St. - 92402/2013 20:16:31.62
24 HR ATM 033861 ATM 861

Transaction #0503
CARD NO: 6418

LOCATION: 1527 2ND AVENUE
SEATTLE WA

CARD NO: XXXXXXXXXXXXXXX6418

DATE 01/05/13 TIME 08:34PM
TERMINAL WA033862

SEQ NBR: 0503 AMT: \$380.00
ATM OWNER FEE \$2.50
TOTAL \$382.50
CHECKING WITHDRAWAL \$191.41
AVAILABLE BALANCE \$191.41
LOCATION: 1527 2ND AVENUE
SEATTLE WA

CARD NO: XXXXXXXXXXXXXXX6418

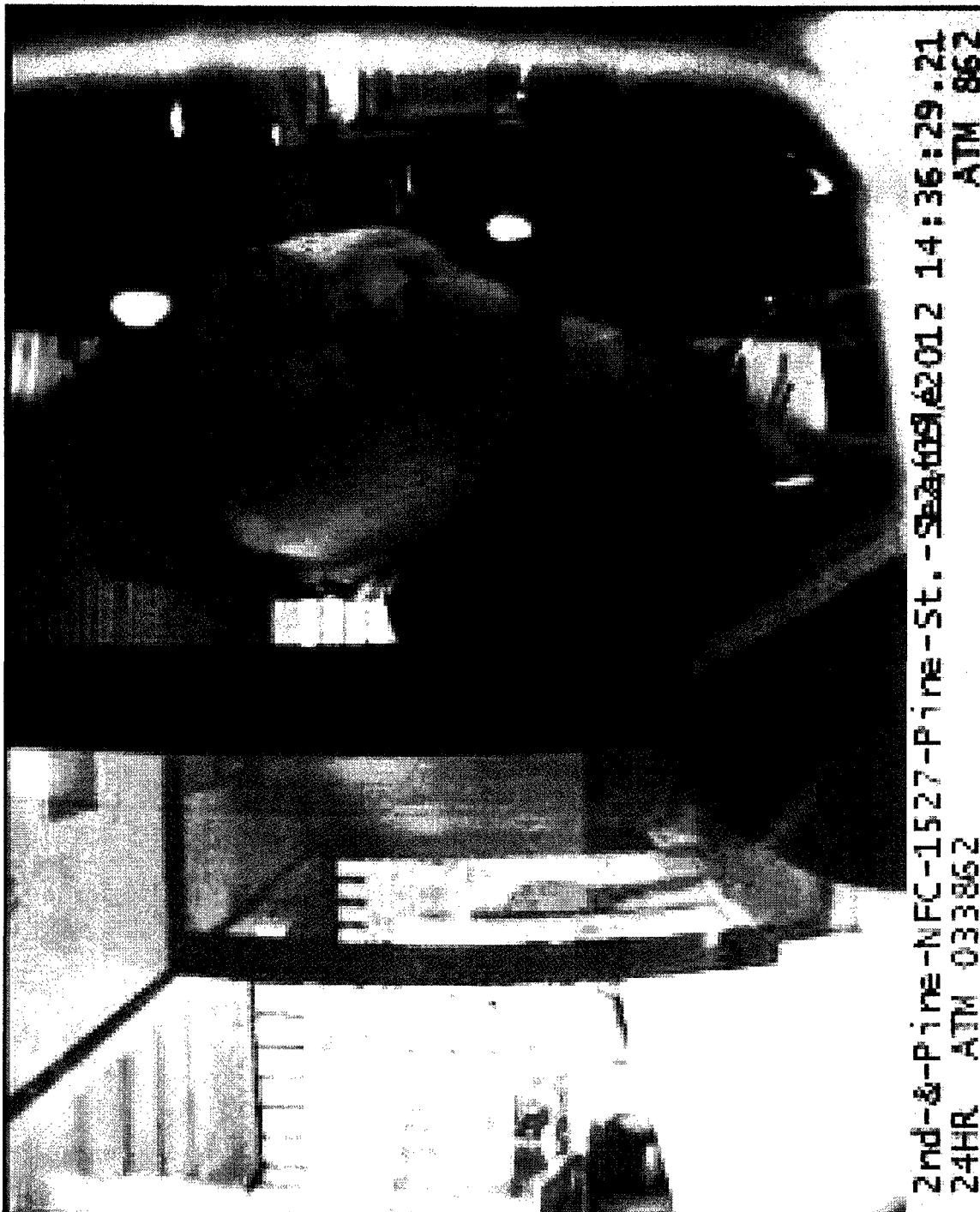
DATE 01/05/13 TIME 08:34PM
TERMINAL WA033862

SEQ NBR: 0503 AMT: \$380.00
ATM OWNER FEE \$2.50
TOTAL



2nd & Pine - NFC-1527-Pine-St. - Seattle, WA 98101 20:34:57.27
24HR ATM 033862

Transaction #0531



Transaction #7886

